BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-113

1 APRIL 1996
Communications

★*TELECOMMUNICATIONS CENTERS AND DATA PROCESSING CENTERS MANAGEMENT*

NOTICE: This publication is available digitally. Contact your Publishing Distribution Office (PDO) for the monthly CD-ROM or access to the bulletin board system. The target date for discontinuing paper publications is December, 1996.

This instruction implements Air Force Policy Directive (AFPD) 33-1, *Command, Control, Communications and Computer (C4) Systems*. This instruction provides procedures and assigns responsibilities for managing telecommunications centers (TCC) and data processing centers (DPC). It does not apply to data processing activities using only small computers for support of the activity's mission. This instruction does not apply to other Federal Supply Group 74 equipment used in an office environment (e.g., electronic copiers). Major commands (MAJCOM), field operating agencies (FOA), and direct operating units (DRU) send one copy of their final supplement to Headquarters Air Force Command, Control, Communications, and Computer Agency, Policy Branch (HQ AFC4A/XPXP), 203 West Losey Street, Room 1065, Scott AFB IL 62225-5233. Refer technical questions about this instruction to HQ AFC4A/SYND, 203 West Losey Street, Room 3065, Scott AFB IL 62225-5233. Refer recommended changes and conflicts between this and other publications on AF Form 847, **Recommendation for Change of Publication**, through channels, to HQ AFC4A/XPXP. Violations of the prohibitions of paragraph 7.1.3 by military members constitute a violation of Article 92, *Uniform Code of Military Justice* (UCMJ), and may result in punishment under the UCMJ. Violations of paragraph 7.1.3 by civilian personnel may result in administrative or other disciplinary action under applicable civilian personnel regulations or instructions. For a listing of references, abbreviations, and acronyms, see attachment 1.

SUMMARY OF REVISIONS

This revision updates the entire document.

Paragraph

Supersedes: AFI 33-113, 30 June 1994.
OPR: HQ AFC4A/SYND (MSgt Robert Cole)

Certified by: HQ USAF/SCXX (Lt Col George L. Fiedler)
Pages: 16/Distribution: F

Section A—The Base Command, Control, Communications, and Computer Systems Officer

1. Commanders:

1.1. The Base C4 Systems Officer (CSO) For Base Wide Systems and the Unit Commander With a DPC:

1.1.1. Makes sure C4 processing equipment and personnel meet the needs of the users.

1.1.2. Makes sure authorized personnel picks up output products or sends them through the base information transfer system (BITS) as security requirements permit.

1.1.3. Decommissions equipment when no longer needed.

1.1.4. Makes and keeps an on-the-job training program.

1.1.5. Sets up a customer education program.

1.1.6. Makes sure destruction facilities meet the needs of the DPC and TCC.

1.1.7. Prepares and coordinates support agreements for all tenants (AFPD 25-2, *Support Agreements*).

1.1.8. Makes sure letters of agreement or memorandums of agreement exist with offices of primary responsibility that have console mode capability.

1.1.9. Implements MAJCOM computer security (COMPUSEC) programs at base level.

Section B—Facility Management

2. Telecommunication and Data Processing Center Managers:

2.1. Set up local procedures for physical and C4 security.

2.2. Set up safety and fire practices.

2.3. Keep environmental conditions according to equipment specifications and set up emergency procedures for environmental equipment failures. TCCs or DPCs that have an energy management control system do not require recording devices.

2.4. Make sure of TCC and DPC equipment room cleanliness.

2.5. Make contingency operations plans.

2.6. Set up a preventive maintenance (PM) schedule. See attachment 2 for a sample PM designation memorandum.

Section C—Operations Management

3. Telecommunication and Data Processing Center Managers:

3.1. Follow guidance and standards as developed by allied communications publications (ACP); Defense Information Systems Agency (DISA) circulars, Joint Army-Navy-Air Force publications (JANAP), MAJCOM, and other applicable directives. **NOTE:** Users may obtain DISA publications by writing to Director, DISA, ATTN: C10-DO3A, 701 S. Courthouse Rd, Arlington VA 22204-2199. Request DISA send you DISA Notice 210-0-1, Index, and DISA Form 117, **Request for Publication.**

3.2. Make procedures for operating computer equipment during severe weather conditions (e.g., thunderstorms within 10 statute miles of an installation, ice storms, high wind conditions, etc.) including contractual liabilities for unique systems.

3.3. Set up local procedures for alternate routing of automatic digital network (AUTODIN) traffic based on local rules in the current DISA operation plan.

3.4. Schedule AUTODIN service interruptions according to DISA Circular 310-D70-30, *DCS AUTODIN Switching Center and Subscriber Operations.*

3.5. Keep master station logs according to DISA Circular 310-D70-30.

3.6. Make sure AUTODIN address indicating group (AIG) case files remain current at all times, to include letters or messages to users advising them of deletion of their AIG if not recapitulated in the appropriate time frame of 13 months. Include NAVCSRF Honolulu HI//N33// as an information addressee in all new, modified, canceled or summary AIGs, if it is not a member of the AIG.

3.7. Send requests for additions, deletions, and changes to routing indicators and plain language addresses to ACP 117s to your MAJCOM for validation. MAJCOMs will reference

AFPD 38-5, *Unit Designations,* when validating proposed plain language address changes to make sure of uniformity of unit designations. **NOTE**: On implementation of the Defense Messaging System (DMS) you will not need to use office symbols as part of the plain language address in ACP 117s.

3.8. Submit requests for mailing address changes according to Air Force Directory 37-135, *Air Force Address Directory.*

3.9. Set up local procedures for MINIMIZE (ACP 121 USSUPP1F [C], *Communications Instructions-General* [U]).

3.10. Set up traffic analysis standards or other measurements to evaluate performance according to local procedures. Send copies of MAJCOM-developed standards to Headquarters United States Air Force, Infrastructure Division (HQ USAF/SCMI), 1250 Air Force Pentagon, Room 5B520, Washington DC 20330-1250, and HQ AFC4A/SYN for consideration in developing Air Force standards.

3.11. Coordinate all AUTODIN system and equipment changes with the C4 planning and implementation activity according to DISA Circular 310-130-1, *Submission of Telecommunications Service Requests.* Send change request to the parent MAJCOM, with information copies to DISA and affected AUTODIN switching center (ASC).

3.12. Use software deficiency reports to identify problems preventing the system from performing its designed functions (see attachment 4). Deficiency reports fall into the following categories:

3.12.1. Emergency Deficiency Reports (Category 1) for problems that result from system failures, security hazards, loss or duplication of data, or other conditions which seriously impact data handling. Send to the applicable software support office via telephone. Follow up with a letter or message to that office and the following information addressees: HQ AFC4A/SYN, the parent MAJCOM, and the Headquarters Standard Systems Group Operating Location-B (HQ SSG OL-B/SDAP, 3580 D Ave, Bldg 201 West, Tinker AFB OK 73145-9155.

3.12.2. TCC Routine Deficiency Reports (Categories 2, 3, and X). Send with a message or letter to the originator's immediate higher headquarters. Send information copies to HQ AFC4A/SYN and HQ SSG OL-B/SDAP. If the MAJCOM is not the immediate higher headquarters, also send an information copy to the parent MAJCOM.

3.13. Customer Support. Develop local procedures for customer visits, user group meetings, customer education programs or questionnaires to make sure customer requirements are being met and the mission requirement is fully supported.

Section D—Software Processing

4. Software Releases. The DPC or TCC manager or the designated representative enters software changes into an operating unit's operational software when applicable software support office releases the software change.

5. Organizational Responsibilities for Deficiency Processing.

5.1. MAJCOMs review and evaluate deficiency reports and send a message to the appropriate software support office to resolve. Include HQ AFC4A/SYN and HQ SSG OL-B/SDAP as information addressees on all correspondence.

5.2. The software support office designs, codes, certifies, and releases software changes in response to emergency deficiencies to the field.

5.3. Units implement software changes on receipt. Within 24 hours of patch implementation, units notify the applicable software support office of patch implementation by sending an operational software implementation notice as shown in attachment 4. Units close a deficiency if it cannot be recreated or it does not recur within 30 days.

Section E—Message Handling and Administrative Procedures

6. Policy, Procedures, and Guidance. ACP 121 USSUP1F, JANAP-128J, *Automatic Digital Network (AUTODIN) Operating Procedures*, and various DISA publications contain specific policies, procedures, and guidance for the operation and management of AUTODIN TCCs.

6.1. Authorized Users of the AUTODIN System. Limit use of AUTODIN to official business that is best sent by electrical transmission. The following non-DoD organizations may use the system under certain conditions:

6.1.1. Specifically designated federal credit unions and military banking facilities operating on military installations originate messages relative to the conduct of their business (e.g., military pay, allotments, records errors, accounting and finance office matters, etc.) in direct support of military personnel at those locations when no commercial record communications exist. Consider requests for approval for this type of service on a case-by-case basis. Send fully justified requests through the base CSO to the installation commander for approval. Send copies through MAJCOM channels to HQ USAF/SCMI for review and comments prior to approval.

6.1.2. Contractors and foreign governments use the system under conditions explained in ACP 121 USSUP1F.

6.1.3. American Red Cross sends administrative and emergency messages pertaining to the death or severe illness of a service member's immediate family. Assign a precedence equal to the priority needed.

7. Message Handling Procedures:

7.1. Incoming Message Processing. TCC personnel:

7.1.1. Process all incoming messages in order of precedence on a first-in-first-out basis. Commanders will not task TCC personnel to pick up messages from originators or deliver messages to addressees location.

7.1.2. Distribute narrative messages based on address, functional address symbol (FAS), or delivery instructions in the first line of text. Units not having a FAS must provide delivery instructions to the TCC.

7.1.3. Do not divulge, release, or publish the contents, purpose, effect, or meaning of messages to any person other than the addressee, the addressee's representative, or a person authorized to accept, forward, or deliver the message. Unauthorized disclosures by military personnel violate Article 92 of the UCMJ and may result in punitive action under the UCMJ. Unauthorized disclosure by civilian personnel may result in administrative or other disciplinary action under applicable civilian personnel regulations or instructions.

7.1.4. Follow local operating procedures for recording the receipt of messages in non-automated TCCs. Use Air Force (AF) Form 3534, **Channel Number Sheet**, for recording channel numbers, if applicable. See attachment 3 for suggested items for operating procedures.

7.1.5. Notify the "action" addressees on receipt of IMMEDIATE and higher precedence messages. If a message management letter is not on file at the TCC, call the organization commander, deputy commander, or the appropriate directorate chief.

7.1.6. Read messages over the telephone when it is imperative to notify an individual about a casualty situation such as a Red Cross message, or when unclassified high precedence messages are routed to an alternate delivery station and distance precludes timely delivery.

7.1.7. Notify the addressee on receipt of an emergency command precedence (ECP) message (e.g., emergency action message [EAM], FLASH, RED and WHITE ROCKET messages).

7.1.8. Distribute one copy of each message to the appropriate 2-letter internal distribution office or single office for an organization. **NOTE***:* Because of the nature and urgency of message traffic that a COMSEC account (CA) receives, direct message release to the CA is authorized. Address CA messages to the local communications unit with a FAS of the CA and its designated six alpha numeric characters.

7.1.9. Use BITS to deliver routine and priority precedence messages not requiring special handling.

7.1.10. Place messages with special handling designators, special delivery instructions, or other caveats restricting distribution in AF Form 3530, **Special or Limited Distribution Message Envelope**, at the TCC and hold for pickup. Do not send through normal delivery channels unless specifically requested by the recipient, and then only as permitted by security constraints. Release immediate and above precedence messages, messages with special designators (such as No Foreign Nationals or Atomic Energy Restricted) and all classified messages requiring receipt in compliance with DoDR 5200-1, *DoD Information Security Program Regulation*, June 1986; AFPD 31-4, *Information Security*, and AFI 31-401, *Managing the Information Security Program* directly to the addressee or designated representatives of the addressee.

7.1.11. Keep AF Form 3531, **Message Delivery Register**, on all messages that require a receipt.

7.1.12. Place unclassified messages in a plain envelope or Optional Form (OF) 65C, **U. S. Government Messenger Envelope**, to send through BITS.

7.1.13. Deliver TOP SECRET messages according to DoDR 5200-1, AFPD 31-4, and AFI 31-401. Deliver TOP SECRET special category (SPECAT) messages according to the instructions for SPECAT. The person authorized to receive the SPECAT message must notify the unit's TOP SECRET control authority of the message receipt. The TCC must place all SPECAT, TOP SECRET, Limited Distribution (LIMDIS), Inspector Distribution (INSPECDIS), and other privacy messages in an AF Form 3530 before effecting delivery.

7.1.14. Deliver "PERSONAL FOR" messages to the individual named or designated representative. The following rules apply to "PERSONAL FOR" messages:

7.1.14.1. Do not re-address.

7.1.14.2. Place in an Air Force Form 3530 and hold for pickup.

7.1.14.3. Do not deliver through normal delivery channels or BITS.

7.1.14.4. Use the caveat "PERSONAL FOR (NAME)" or "PERSONAL FOR (NAME) FROM (NAME)".

7.1.15. Place drug testing messages received with the phrase "DBMS EYES ONLY" at the end of the classification line in an AF Form 3530 before delivery.

7.1.16. Place Critical Nuclear Weapon Design Information (CNWDI), Cryptographic, Restricted Data, or other designators indicating special handling in the text following the security classification. Place markings for RESTRICTED DATA-ATOMIC ENERGY ACT 1954, and FORMERLY RESTRICTED DATA ATOMIC ENERGY ACT on the message as shown in DoDR 5200-1, AFPD 31-4, and AFI 31-401.

7.1.17. Use the INSPECDIS designator within and between Air Force activities only for Inspector General activities. It flags the message for distribution only to the office addressed and for viewing only by Inspector General personnel.

7.1.18. Receive Electronic Warfare Integrated Reprogramming (EWIR) messages on a diskette which does not contain any other messages. Do not attempt to change or correct EWIR messages. **NOTE***:* EWIR messages are both real world (PACER WARE) and test (SERENE BYTE).

7.1.19. General Messages . General messages addressed to customers (ALFOODACT, etc.) do not require logging or retention past that of other regular message traffic. Log general messages addressed to the TCC (e.g., JAFPUB, ALMILACT, NETCONMSG, etc.) on AF Form 3532, **General Message Record**, and file sequentially. The first general message of each year provides disposition and destruction authority for the previous year's general messages. Track general messages chronologically for the current year.

7.1.20. Find the local FAS address with the customer-provided list of AIG local addresses.

7.1.21. Keep a current list of individuals authorized to pick-up and receive messages.

7.2. Outgoing Message Processing. TCC personnel:

7.2.1. Protect information against loss or compromise.

7.2.2. Process messages first-in-first-out by precedence. Process high precedence messages expediently and provide status to supervisory personnel.

7.2.3. Assign station serial numbers (SSN) manually if equipment does not automatically assign them. Use AF Form 3533, **COMMCEN Message Register**, to log originated messages when applicable. Close out the form daily. When starting a new register, bring forward the next unused consecutive SSN from the previous register.

7.2.4. Assign routing indicators, if applicable.

7.2.5. Proofread the entire message if prepared manually.

7.2.6. Verify that the table of contents (TOC) cycle redundancy check (CRC) number on the releasing document matches the internal TOC CRC on the diskette before transmission.

7.2.7. Write the time of transmission if equipment does not have an automatic journal or log.

7.2.8. File messages sequentially by SSN, time of file, or date-time-group per local procedures.

7.2.9. Keep magnetic tape reels and diskettes for 72 hours and then return to originator. TCCs with automatic retrieval capability may return tapes and diskettes to originator after processing.

7.2.10. The releaser's organization reproduces additional copies of outgoing messages prior to delivery to the TCC. Delivery to ZEN addresses is the sole responsibility of the message originator. Unless specifically directed by local policy, the TCC will not reproduce additional copies of outgoing messages for customer related responsibilities. Do not provide originators with comeback or file copies. TCCs may self-address operational readiness inspection (ORI) exercise messages into AUTODIN to evaluate ability to manually process traffic by using the following criteria:

7.2.10.1. Give the affected ASC 8 hours prior notification, by message, of the test introduction of self-addressed message traffic.

7.2.10.2. The notification message will consist of date and time of test start, approximate number of messages to send, name and telephone number of ORI point of contact, and name of TCC getting evaluated.

7.2.10.3. Assign a block of SSNs to remote terminals to identify specific remotes according to local instructions.

7.2.10.4. Submit high volume message inputs according to DISA Circular 310-D70-30.

7.2.11. Keep handling of SPECAT, LIMDIS, and other special handling messages to the minimum personnel needed to process and package the product according to governing regulations. TCC personnel must set apart the following types of messages and take the actions indicated. **NOTE***:* Destroy special handling message residue (SPECAT, etc.) after transmission or return it to the originator as local conditions warrant. If returned to the originator, package and account for the material according to DoDR 5200-1, AFPD 31-4, and AFI 31-401.

7.2.11.1. ECP, EAM, FLASH, RED, AND WHITE ROCKET. Establish handling procedures which:

7.2.11.1.1. Process these messages with minimal pre-logging. Fill in logs after transmission.

7.2.11.1.2. Advise the originator of delays or anticipated delays in message processing.

7.2.11.2. Limit handling and viewing of SPECAT-designated messages to properly cleared and authorized personnel. Require direct processing of SPECAT messages between the releasing or distribution office and the TCC, or between the TCC and the addressees unless local conditions call for intermediate handling. Require special clearances and access for personnel at such intermediate points to handle the SPECAT material. Activities that need to send or receive SPECAT messages give the servicing TCC a special access list of personnel who may sign for SPECAT messages. Follow the SPECAT designator with "EXCLUSIVE FOR (name)" or by a specific identification, acronym, or code word identifying the project or subject. Refer to ACP 121 USSUP1F for further guidance. Types of SPECAT messages:

7.2.11.2.1. EXCLUSIVE FOR. Example: S E C R E T SPECAT EXCLUSIVE FOR GEN SMITH. **NOTE***:* Do not use terms or phrases such as "EYES ONLY," "PERSONAL FOR," etc., on SPECAT messages.

7.2.11.2.2. Single Integrated Operational Plan Extremely Sensitive Information (SIOP-ESI), governed by AFI 10-1102, *Safeguarding the Single Integrated Operational Plan (SIOP)*. Example: T O P S E C R E T SPECAT SIOP-ESI.

7.2.11.3. Other special handling message types:

7.2.11.3.1. LIMDIS Designators. Designates classified messages that must have limited distribution and special handling in user channels (paragraph 7.1.13). Stamp or block letter "LIMDIS" on the first page of LIMDIS designated messages when processing.

7.2.11.3.2. TOP SECRET.

7.2.11.3.3. Personal For. General or Flag officers and civilians of equivalent rank originate "PERSONAL FOR" messages. The caveat "PERSONAL FOR" means you must protect the privacy of the message.

7.2.11.3.4. Drug Testing.

7.2.11.3.5. CNWDI.

7.2.11.3.6. INSPECDIS.

7.2.11.3.7. EWIR. Do not retain the media used for transmission or associated printouts for more than three days after transmission. Return all products to the originator on completion of service action or retransmission requests.

7.3. Correcting message preparation errors.

7.3.1. Major errors preclude transmission of the message (i.e., incomplete or incorrect address element which the TCC cannot correct, security mismatch, no releaser's signature, improperly prepared or unreadable diskettes, TOC/CRC mismatch, etc.). In these cases, the TCC operator follows local procedures for contacting releasing officials or fills out a DD Form 1503, **Message Correction Notice**, and promptly returns Routine messages with the form to the releasing officials for reaccomplishment or correction. For

Priority or higher precedence messages, the operator immediately notifies the releasing official or agency to initiate corrections. If unable to reach the releasing official follow local procedures for notification.

7.3.2. Minor errors do not preclude further processing of the message. The operator coordinates with the releasing official or message drafter, if necessary, to resolve specific preparation errors. The operator then processes and transmits the message and follows local procedures for notifying the originator or sends the originator a DD Form 1503.

7.4. Use service messages for exchanging information to speed up, correct, clarify, report, or ease the flow of message traffic. Also use them to deal with anticipated workloads of an unusual nature, SPECAT information, or information requiring special handling, the adjustment of procedural discrepancies, or changes to available facilities. All service messages must conform to rules of transmission and COMSEC. Use only authorized and appropriate operating signals and prosigns for service messages. Refer to ACPs 127 USSUP1H, *Communications Instructions Tape Relay Procedures;* 131 USSUP1D, *Communications Instructions Operating Signals;* and JANAP 128J for further guidance.

Section F—Automated Message Processing Exchange Operations

8. Introduction. The Automated Message Processing Exchange (AMPE) does various processing jobs including automatic message formatting and routing, automatically determining incoming distribution, and switching messages to and from AUTODIN, other AMPEs, and its own tributary stations. The AMPE also serves as the sole link between the ASC and its tributary stations.

8.1. AMPE remote terminals and tributary stations vary in configuration from a receive-only low speed printer to a large computer terminal, optical character reader, magnetic tape terminal, keyboard video display terminal, or other input/output equipment.

8.2. Customer-operated tributary stations usually support a dedicated mission and possibly one or two other customers. Their work includes only those C4 systems functions necessary to send and receive the tributary station's information. They rely on the AMPE as a network control station.

8.3. Other tributary stations may support a single dedicated user, multiple users, or may act as TCC.

8.4. C4 Personnel operating remote terminals must:

8.4.1. Protect information against loss or compromise.

8.4.2. Carry out security practices.

8.4.3. Follow communications security (COMSEC) procedures.

8.4.4. Aid the TCC in obtaining a unique routing indicator.

8.4.5. Furnish the TCC with copies of current AIGs used to transmit or receive messages.

8.4.6. Publish and coordinate local procedures with the AMPE to cover the processing of service messages by those remotes manned by Air Force specialty code (AFSC) Communications Computer Systems Operations (3C0X1) personnel. The host AMPE personnel take care of all service actions for remotes manned by non-AFSC 3C0X1 personnel.

8.5. The AMPE acts as the network control station for its remote tributary stations. The network control station personnel must:

8.5.1. Set up a formal system of network control messages.

8.5.2. Furnish technical assistance and training.

8.5.3. Oversee the operational performance of its tributary and remote stations, help in the correction of deficiencies, and complete a monthly performance summary using ACP 121 USSUP1F, Annex C, for guidance. Include repetitive information in a one-time brochure. Distribute the communications operating performance summary to all tributary and remote stations and the MAJCOM.

8.5.3.1. Maintain system control to minimize operational impact of failures to tributaries, the AMPE, or the connected ASC.

8.5.3.2. Set up and maintain a workable alternate routing plan to protect tributary stations from loss or excessive delay of information during equipment or circuit outages.

8.5.3.3. Make and maintain a customer education package for distribution to all customer-operated terminals.

8.6. Excessive queues may generate a requirement for operator intervention. Queues consist of messages awaiting transmission to each channel and is defined in terms of message numbers and line blocks. Take one of the following actions immediately when excessive queues exist:

8.6.1. Implement established alternate routing procedures.

8.6.2. Extract messages from the queue and place them in temporary storage (intercept storage). Restrictions on the use of intercept storage follow:

8.6.2.1. Do not store EMERGENCY COMMAND precedence (YY) and FLASH precedence (ZZ) messages on intercept unless they are routed to part-time stations that you cannot reach or a system has failed. Part-time stations must establish procedures to make sure their customers can receive high precedence messages.

8.6.2.2. Do not store more than 250 messages or 14,000 line blocks on an intercept storage tape.

8.6.2.3. Read intercepted messages into the system as soon as possible.

8.6.2.4. Initiate input inhibit procedures.

Section G—Message Terminal Operations

9. Introduction. The message terminal (MT) does various processing jobs including automatic message formatting and routing, automatically determining incoming distribution, and switching messages to and from AUTODIN, other MTs, and its own tributary stations.

9.1. Remote terminals and tributary stations are PC-based platforms and vary in configuration.

9.2. Customer-operated tributary stations usually support a dedicated mission and possibly one or two other customers. Their work includes only those C4 systems functions necessary to send and receive the tributary station's information. They rely on the MT as a network control station.

9.3. Other tributary stations may support a single dedicated user, multiple users, or may act as TCC.

9.4. C4 Personnel operating remote terminals must:

9.4.1. Protect information against loss or compromise.

9.4.2. Follow security practices.

9.4.3. Follow communications security (COMSEC) procedures.

9.4.4. Help the TCC in obtaining a unique routing indicator.

9.4.5. Furnish the TCC with copies of current AIGs used to transmit or receive messages.

9.4.6. Publish and coordinate local procedures with the MT to cover the processing of service messages by those remotes manned by AFSC 3C0X1 personnel. The host MT personnel take care of all service actions for remotes manned by non-AFSC 3C0X1 personnel.

9.5. The MT acts as the network control station for its remote tributary stations. The network control station personnel must:

9.5.1. Set up a formal system of network control messages.

9.5.2. Give technical assistance and training.

9.5.3. Maintain system control to minimize operational impact of failures to tributaries, the MT, or the connected ASC.

9.5.4. Set up and keep a workable alternate routing plan to protect tributary stations from loss or excessive delay of information during equipment or circuit outages.

9.5.5. Develop and maintain a customer education package for distribution to all customer-operated terminals.

9.5.6. Keep a continuity folder with system configurations, crossfeeds from HQ SSG OL-B/SDAP, and appropriate reference materials and operating instructions (OIs).

Section H—Storage Media Management

10. Storage Media Libraries:

10.1. The TCC or DPC manager must set up procedures that cover control, security, and upkeep of all storage media.

10.1.1. External tape or disk identification. Use magnetic media labels and guidelines as prescribed in DISA Circular 310-D70-30 and applicable Air Force Systems Security Instructions (AFSSI) and Air Force Systems Security Memorandums (AFSSM). Make sure of effective management and control by putting the following items on the outside of the tape reel, floppy disk, disk pack or cartridge:

10.1.1.1. *Organizational identification.

10.1.1.2. *Reel or disk pack/cartridge number (tape reel or disk pack cartridge only).

10.1.1.3. *Recording density.

10.1.1.4. *Security classification.

10.1.1.5. *Acquisition date (tape reel or disk pack cartridge only).

10.1.1.6. *Operating system (floppy disk only).

10.1.1.7. Physical characteristics (length, width, hub size, number of disks, compatible drive, etc.).

10.1.1.8. Usage record (including cleaning).

10.1.1.9. Error reports.

10.1.1.10. Final disposition.

10.1.1.11. Physical location.

NOTE: Place information marked with an asterisk (*) on the outside of the magnetic medium (e.g., tape reel, disk pack cartridge, or floppy disk). The TCC manager stores all other information elsewhere.

10.1.2. Internal Tape Identification. The internal identification of tapes is software-controlled information. Include the title, file number, reel of file, date written, purge date (date the data becomes obsolete and the tape may be reused), classification, and declassification instructions in this information.

10.2. Cleaning or Rehabilitation Cycle. Keep a record, by reel, pack, or cartridge number, of the date serviced. Turn in items no longer usable to the local Defense Property Disposal Agency (DoD Manual 4160-21, *Defense Reutilization and Marketing Manual*, March 1990). Degauss all items with classified or personal information and remove any labels or documentation attached which could reveal the previous contents of the degaussed tape or its sensitivity before turning them in. AFSSI 4100, *(C) Communications Security Program (U)*, along with various AFSSIs and AFSSMs provide guidance.

10.3. Inventory Accountability. Library records provide listings of the media on hand in the library, those temporarily out for cleaning or rehabilitation, magnetic media shipped out for use elsewhere, those on hand belonging to another center or organization, and any media awaiting disposition. Control and inventory of classified magnetic media in the library is prescribed in DoDR 5200-1, AFPD 31-4, AFI 31-401, and AFSSI 4100.

10.4. Care, Handling, and Maintenance of Magnetic Tape. Personnel who work with magnetic media must maintain and use them according to local instructions.

10.5. Shipping Magnetic Tapes:

10.5.1. Make sure the outer container is water resistant and strong enough to protect the tape from damage.

10.5.2. Mark the outer container with--**FRAGILE, MAGNETIC TAPE, KEEP AWAY FROM ELECTRIC MOTORS, SCANNING DEVICES, AND MAGNETICS--**or use an OF 85, **Fragile - Magnetic Tape Label**.

10.6. Classified Magnetic Media. Mark, ship, and safeguard classified magnetic media according to DoDR 5200-1, AFPD 31-4, AFI 31-401, and AFSSI 4100.

10.7. Immediate Access Storage (IAS) Management:

10.7.1. Development centers set up disk management standards governing programs and files allowed to reside on disks.

10.7.2. Keep only necessary programs and files on disks.

10.7.3. Backup critical programs, disk resident files, system software routines, production programs, and data files on tape and store in a secure location away from the facility.

10.7.4. Appoint an IAS manager for each installed computer system as required. Furnish guidelines and set up controls within TCC and DPC operations for the following areas:

10.7.4.1. Load and remove programs and files as needed.

10.7.4.2. Verify validity of program versions and backups.

10.7.4.3. Oversee the status of checker boarding and schedule compacting procedures.

10.7.4.4. Run disk analysis programs to check disk use.

10.7.4.5. Apply procedures for care and control of IAS hardware.

10.8. Storing Magnetic Media:

10.8.1. On-site storage. Store computer programs and data files in a fire-retardant vault area or in fire-retardant cabinets (when feasible).

10.8.2. Off-site storage. Keep selected files, to include operations programs, system builds, data base directories, etc., in a secure area physically separated from the TCC or DPC. Select the off-site storage location based on its proximity to the TCC or DPC, the temperature and humidity, and the physical security of the building. Place a priority schedule for recreating files, as well as those products specified in other areas of this publication, at the off-site storage location.

11. Forms Prescribed. This instruction prescribes AF Forms 3530, 3531, 3532, 3533, and 3534, DD Form 1503, and OF 85.

JOHN S. FAIRFIELD, Lt General, USAF
DCS/Command,Control, Communications, and Computers

GLOSSARY OF REFERENCES, ABBREVIATIONS, AND ACRONYMS

References

JANAP-128J, *Automatic Digital Network (AUTODIN) Operating Procedure*
DoDR 5200-1, *DoD Information Security Program Regulation*, June 1986
DoDM 4160-21, *Defense Reutilization and Marketing Manual*, March 1990
AFPD 25-2, *Support Agreements*
AFPD 31-4, *Information Security*
AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*
AFPD 38-5, *Unit Designations*
AFI 10-1102, *Safeguarding The Single Integrated Operational Plan (SIOP)*
AFI 31-401, *Managing the Information Security Program*
AFI 37-124, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections*
AFDIR 37-135, *Air Force Address Directory*
AFSSI 4100, *(C) Communications Security Program (U)*
ACP 121 USSUP1F (C), *Communications Instructions-General (U)*
ACP 127 USSUP1H, *Communications Instructions Tape Relay Procedures*
ACP 131D, *Communication Instructions Operating Signals*
DISA Circular 310-D70-30, *DCS AUTODIN Switching Center and Subscriber Operations*
DISA Circular 310-130-1, *Submission of Telecommunications Service Requests*

Abbreviations and Acronyms

ACP−Allied Communications Publication
AF−Air Force
AFI−Air Force Instruction
AFPD−Air Force Policy Directive
AFR−Air Force Regulation
AFSC−Air Force Specialty Code
AFSSI−Air Force Systems Security Instruction
AFSSM−Air Force Systems Security Memorandum
AIG−Address Indicating Group
AMPE−Automated Message Processing Exchange
ASC−AUTODIN Switching Center
AUTODIN−Automatic Digital Network
BITS−Base Information Transfer System
CA−COMSEC Account
C4−Command, Control, Communications, and Computers
CNWDI−Critical Nuclear Weapon Design Information
COMPUSEC−Computer Security
COMSEC−Communications Security
CRC−Cycle Redundancy Check
CSO−C4 Systems Officer
CSP−Communications System Processor
DIREP−Difficulty Report
DISA−Defense Information Systems Agency
DMS−Defense Messaging System
DoD−Department of Defense
DPC−Data Processing Center
DRU−Direct Reporting Unit
EAM−Emergency Action Message
ECO−Equipment Control Officer
ECP−Emergency Command Precedence
EIW−Engineering Installation Wing
EWIR−Electronic Warfare Integrated Reprogramming

FAS−Functional Address Symbol
FOA−Field Operating Agency
HQ AFC4A−Headquarters Air Force C4 Agency
HQ AIA−Headquarters Air Intelligence Agency
HQ USAF−Headquarters United States Air Force
IAS−Immediate Access Storage
INSPECDIS−Inspector Distribution
JANAP−Joint Army-Navy-Air Force Publication
LIMDIS−Limited Distribution
MAJCOM−Major Command
MT−Message Terminal
OF−Optional Form
OI−Operating Instruction
ORI−Operational Readiness Inspection
PM−Preventive Maintenance
SIOP-ESI Information−Single Integrated Operation Plan-Extremely Sensitive
SPECAT−Special Category
SRT−Standard Remote Terminal
SSN−Station Serial Number
TCC−Telecommunications Center
TOC−Table of Contents
UCMJ−Uniform Code of Military Justice
YY−Emergency Command Precedence
ZZ−Flash Precedence

SAMPLE MEMORANDUM, DESIGNATION OF PREVENTIVE MAINTENANCE

MEMORANDUM FOR (Vendor, Local Branch Address)

FROM:

SUBJECT: Preventive Maintenance Schedule and Designation of Principal Period of Maintenance, (Vendor/
GSA__________, Contract #__________)

1. Reference (paragraph or article), (special item or section), subject contract, with regard to maintenance of data processing equipment.

2. Effective (date), the principal period of maintenance for this installation is established as (hours of the day and days of the week). The vendor will perform preventive maintenance on the equipment listed on delivery order(s) (number(s) and date), or as listed here, beginning at (time of day) and ending at (time of day) on (days) of each week.

3. Mutual agreement to this schedule is indicated below.

FOR THE AIR FORCE FOR

(Signature of ECO) (Vendor)

(Signature of Representative)

SUGGESTED ITEMS FOR OPERATING PROCEDURES

A3.1. Temperature and humidity controls.

A3.2. Magnetic media controls.

A3.3. Management of the remote processing facilities.

A3.4. Physical security and accountability.

A3.5. Duties of equipment custodian and equipment control officer.

A3.6. Shift activity and turnover log.

A3.7. Control of difficulty reports (DIREP) and software modification reports.

A3.8. Power-up or power-down procedures (clear with vendor engineer).

A3.9. Control and distribution of system advisory notices and DIREP status reports.

A3.10. Housekeeping to include cleaning schedules, methods, etc.

A3.11. Control and handling of systems software releases and modifications. Include suspense dates. Furnish for necessary advice and distribution to functional users.

A3.12. Classified processing. Include disconnect procedures for remote terminals (including dial-ups), marking, control, storage, and disposal of input, output, and waste.

A3.13. Personal data subject to the Privacy Act of 1974.

A3.14. Control of paper and forms. Include:
A3.14.1. Inventory.
A3.14.2. Reorder.
A3.14.3. Actions for unusables.
A3.14.4. Conditioning of supplies prior to use.
A3.14.5. Control of special forms (e.g., treasury checks, bonds, etc.).

A3.15. Internal training. Appoint an on-the-job training monitor, as required.

A3.16. Maintenance of automatic data processing equipment:
A3.16.1. Preventive maintenance (PM) schedules. Record PM not done on schedule.
A3.16.2. Reporting of excessive downtime.
A3.16.3. Other maintenance.
A3.16.4. Maintaining magnetic media cleaners.

A3.17. System initialization procedures.

A3.18. Severe weather conditions.

A3.19. Production distribution center.

A3.20. Products requiring special handling (e.g., payroll checks, SPECAT, classified, high precedence, etc.).

A3.21. Time checks.

A3.22. Procedures and analysis function.

A3.23. Customer education and support to include customer visits and customer satisfaction surveys.

A3.24. Service messages.

A3.25. Message tracer action.

A3.26. Unit computer security officer and terminal area security officer duties.

A3.27. Procedures for the control of remote terminal access to include dial-ups. Also include password generation, distribution, and control.

A3.28. Status reporting.

A3.29. Service calls for maintenance.

A3.30. Contingency and catastrophic failures. Facility emergency plans cover:
A3.30.1. Alert or recall.
A3.30.2. Protection or disposal of classified information and equipment.
A3.30.3. Fire emergency and prevention.
A3.30.4. Site environmental failure.
A3.30.5. Identification of emergency reporting.
A3.30.6. Bomb threats.
A3.30.7. Evacuation.

A3.31. Duties of the data base administrator functions, to include transaction interface processor management, network management, and data base management.

A3.32. Local system security incident reporting to include unsuccessful attempts to access the system, erasure or destruction of stored data, etc.

A3.33. Automated and manual audit trails. Include minimum actions recorded, checking, and retention.

A3.34. Marking and control of programs.

A3.35. Off-site storage. Include security, environment, storage, updating, and inventory procedures.

A3.36. Duties of the magnetic storage librarian function.

A3.37. Duties and responsibilities of shift supervisor or leader.

SOFTWARE DEFICIENCY REPORT

A4.1. Categories of Deficiencies. (The reporting requirements in this attachment are exempt from licensing according to AFI 37-124, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections*.)

A4.1.1. Category 1 Problem. An on-line program problem which seriously jeopardizes traffic handling capability or impairs system integrity. Generally, problems assigned this classification involve those which reduce the system capability for maintaining message integrity, create security or lost message hazards, generate on-line or off-line duplicate messages, and cause computer failures which stagnate traffic.

A4.1.2. Category 2 Problem. A program problem which affects the on-line system. However, it does not jeopardize traffic handling or impair system integrity. Normally, Category 2 problems involve situations and conditions that create an additional workload on system operations but do not warrant immediate relief.

A4.1.3. Category 3 Problem. Any program problem which affects off-line operations, excluding off-line recovery problems which fall under Category 1 criteria.

A4.1.4. Category X Problem. This category is reserved for those problems which are unidentifiable as Category 1, 2, or 3. Usually, such problems will be resolved by determination of specifications, documentation changes, procedural changes, change to operator error and closed, or removed as a problem and submitted by the originating agency as a recommended enhancement for those areas which involve elimination of operator problems or irritants.

Figure A4.1. Operational Software Deficiency Report (Categories 2, 3, and X):

From: OPERATING UNIT COMMANDER OR OPERATIONS OFFICER

TO: OPERATING UNIT'S HEADQUARTERS

INFO: HQ ESC HANSCOM AFB MA//CV//

HQ SSG OL-B TINKER AFB OK//SDA/SDAP//

HQ AFC4A SCOTT AFB IL//SYN//

DIRUSAISSDC-H FT HUACHUCA AZ//ASQBI-HSA// (standard remote terminal [SRT] system only)

HQ AIA KELLY AFB TX//IND// (communications system processor [CSP]system only)

(Other applicable addressees using similar systems, if appropriate.)

(CLASSIFICATION)

SUBJECT: OPERATIONAL SOFTWARE DEFICIENCY REPORT

REQUEST YOU TAKE ACTION TO ANALYZE AND RESOLVE THE FOLLOWING SUSPECTED OPERATIONAL SOFTWARE DEFICIENCY:

A. COMPUTER SYSTEM TITLE:

B. DEFICIENCY PRIORITY: (2,3, AND X ROUTINE)

C. EXPLANATION OF DEFICIENCY:

D. RECOMMENDATION FOR RESOLUTION OF DEFICIENCY:

E. REMARKS: (EQUIPMENT TYPES, COORDINATION AFFECTED, ETC.)

F. NAME, GRADE, PHONE NUMBER, AND TITLE OF ACTION OFFICE.

Figure A4.2. Operational Software Deficiency Report for Category 1:

FROM: OPERATING UNIT COMMANDER OR OPERATIONS OFFICER

TO: DIRUSAISSDC-H FT HUACHUCA AZ//ASQBI-HSA// (SRT systems only)

HQ AIA KELLY AFB TX//IND// (CSP systems only)

HQ ESC HANSCOM AFB MA//CV//

INFO: HQ SSG OL-B TINKER AFB OK//SDA/SDAP//

HQ AFC4A SCOTT AFB IL//SYN//

OPERATIONAL UNIT'S MAJCOM HEADQUARTERS

(Other applicable addressees using similar systems if appropriate)

(CLASSIFICATION)

SUBJECT: OPERATIONAL SOFTWARE DEFICIENCY REPORT

REQUEST YOU TAKE ACTION TO ANALYZE AND RESOLVE THE FOLLOWING SUSPECTED OPERATIONAL SOFTWARE DEFICIENCY:

A. COMPUTER SYSTEM TITLE:

B. DEFICIENCY PRIORITY: (EMERGENCY)

C. EXPLANATION OF DEFICIENCY:

D. RECOMMENDATION FOR RESOLUTION OF DEFICIENCY:

E. REMARKS: (EQUIPMENT TYPES, COORDINATION AFFECTED, ETC.)

Figure A4.3. Operational Software Implementation Notice:

FROM: OPERATING UNIT COMMANDER OR OPERATIONS OFFICER

TO: DIRUSAISSDC-H FT HUACHUCA AZ//ASQBI-HSA// (SRT systems only)

HQ AIA KELLY AFB TX//IND// (CSP systems only)

HQ ESC HANSCOM AFB MA//CV//

HQ SSG OL-B TINKER AFB OK//SDA/SDAP//

INFO: HQ AFC4A SCOTT AFB IL//SYN//

OPERATIONAL UNIT'S MAJCOM HEADQUARTERS

(Other applicable addressees using similar systems, if appropriate)

(CLASSIFICATION)

SUBJECT: OPERATIONAL SOFTWARE IMPLEMENTATION NOTICE

OPERATIONAL SOFTWARE WAS SUCCESSFULLY IMPLEMENTED AND DETAILS ARE AS FOLLOWS:

A. COMPUTER SYSTEM TITLE:

B. SOFTWARE IDENTIFICATION: (SOFTWARE CONFIGURATION DESIGNATOR)

C. JULIAN DATE AND TIME IMPLEMENTED:

D. DEFICIENCY NUMBER CLOSED:

E. REMARKS: (EQUIPMENT TYPES, COORDINATION AFFECTED, ETC.)

NOTE: Notices submitted to close reported deficiencies not adequately documented, have not recurred within 30 days, or not recreated, have as their subject “Deficiency Closure Notice” and written to describe the “Computer System Title,” the “Deficiency Number Closed,” and the explanation that the “Deficiency has not recurred for 30 days and was not recreated.”